

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

FILED
RICHARD W. NAGEL
CLERK OF COURT

1/4/24

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

)

Case No.

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WEST. DIV. DAYTON

Certain Cellular Tower Information in Dayton, Ohio

)

3:24-mj-14

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in various Districts of the United States, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC s. 2114(a)	robbery of a postal carrier

The application is based on these facts:

See attached affidavit of Joseph Rossiter

Continued on the attached sheet.

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Joseph Rossiter
Applicant's signature

Joseph Rossiter, US Postal Inspector

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by reliable electronic means
-- namely, telephone _____

Date: 1/4/24

City and state: Dayton, Ohio

Peter B. Silvain, Jr.
United States Magistrate Judge



**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, **Joseph L. Rossiter**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant for records and information associated with certain cellular towers (“cell towers”) that is in the possession, custody, and/or control of:

- a. T-Mobile USA, Inc., a wireless telephone service provider headquartered at 4 Sylvan Way, Parisppany, NJ 07054;
- b. AT&T Inc., a wireless telephone service provider headquartered at 11760 US Hwy 1, Ste. 600, N. Palm Beach, FL 33408;
- c. US Cellular, a cellular service provider headquartered at 8410 West Bryn Mawr Ave., Chicago, IL 60631; and
- d. Verizon Wireless, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, NJ 07921;

(collectively, the “PROVIDERS”). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require PROVIDERS to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a United States Postal Inspector, having been so employed since May 2016. I am presently assigned to the Cincinnati Field Office, Pittsburgh Division of the United States

Postal Inspection Service (USPIS) with investigative responsibility for southwest Ohio and northern Kentucky. I have gained experience through completion of the Basic Inspector Training (BIT) in May of 2016. During BIT training, I was instructed in all phases of criminal investigation, such as criminal law, search and seizure, field enforcement techniques, firearms proficiency, drug and narcotics identification, drug and narcotics field testing, interviewing, and evidence collection. Since May 2016, I have worked with various federal, state, and local law enforcement agencies in the prosecution of crimes involving the U.S. Mail and the U.S. Postal Service including but not limited to mail theft, burglaries, robberies, homicides, and mailed narcotics.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that unknown persons have committed a violation of Title 18, United States Code, Section 2114(a) (assault on a person having lawful charge, control, or custody of any mail matter, or of any money, or other property of the United States, with intent to rob, steal, or purloin such mail matter, money or other property of the United States). There is also probable cause to search the information described in Attachment A for evidence of this crime as further described in Attachment B.

PROBABLE CAUSE

5. On or about December 18, 2023, at approximately 10:25 A.M., a United States Postal Service (USPS) Letter Carrier was delivering mail on foot near 4808 Marburn Avenue in

Dayton, Ohio, when an unknown male (hereinafter “the suspect”) approached the USPS Letter Carrier. The suspect displayed a firearm and demanded the bag of the USPS Letter Carrier. The USPS Letter Carrier complied with this tacit threat and surrendered to the suspect the mail bag, which contained U.S. Mail. The suspect also took the USPS Letter Carrier’s USPS Scanner. After taking these items, the suspect then fled on foot to a waiting grey sedan that was also parked on Marburn Avenue in Dayton, Ohio.

a. The USPS Letter Carrier attempted to return to his USPS Vehicle, which was parked in the vicinity of 1350 Honeybee Drive in Dayton, Ohio. As the USPS Letter Carrier turned north to Honeybee Drive from Marburn Avenue, the USPS Letter Carrier noticed that the suspect was now trying to gain access to the postal vehicle of the USPS Letter Carrier.

b. The USPS Letter Carrier immediately turned around and headed south on Marburn Avenue, walking towards a utility worker who had parked near the dead end of Honeybee Drive. As the USPS Letter Carrier approached the utility worker, the USPS Letter Carrier heard what sounded like two gunshots fired from the vicinity of his USPS vehicle. The utility worker allowed the USPS Letter Carrier to enter the utility worker’s vehicle, and they called 911.

c. The police from Trotwood, Ohio (hereinafter “TPD”) responded to the scene of the robbery and found two bullet holes in the back of the USPS vehicle. TPD recovered one bullet at the scene. USPIS searched the USPS vehicle and its contents again later that date and recovered a second bullet lodged in a mail tub.

6. On December 18, 2023, Postal Inspectors obtained video surveillance from a residence near the location of the robbery – namely, the 1200 block of Honeybee Drive at approximately 10:23 A.M. The surveillance captured a person similar in description to the

suspect with his arms in the vicinity of the license plate area of a grey Buick sedan. (Based on my training and experience, I know that individuals involved in mail thefts often use getaway vehicles to which they affix stolen or altered license plates. Consistent with that modus operandi, I believe that the suspect was tampering with or altering the plates on the Buick to conceal the identity of its owner.) The video then captured the suspect briefly enter the passenger seat of the Sedan, exit the vehicle, and then walk in the direction of the USPS letter carrier. The sedan then backed up and drove in the direction of the USPS Letter Carrier. These events occurred moments before the robbery. Given the suspect's presence at this vehicle and his later flight in it, I believe that, with the help of an accomplice (namely, the sedan's driver), he used this car to facilitate the robbery.

7. Since January 2022, I have investigated or assisted in the investigation of over 25 robberies of USPS Letter Carriers. In every investigation to date, cellular telephones and their related data have been critical in identifying suspects as well as their co-conspirators. Even though victim letter carriers often never saw robbers in possession of cellular telephones, subsequent investigation of these incidents revealed that the assailants, in fact, carried such devices to coordinate with one another before, during, and after the attacks. For instance:

a. On August 17, 2022, in Covington, Kentucky, a suspect robbed a USPS Letter Carrier of his arrow key while on his route. During the investigation, USPIS identified the suspect and were able to obtain his cellular device. The cellular device was downloaded and revealed that, on the date of the robbery, the suspect used his cellular device to text with conspirators when he completed the robbery, to arrange for the pickup of the stolen key, and to coordinate payment for the robbery. In short, the robber had a cellular device with him during the robbery and used it to facilitate the crime.

b. On or about November 26, 2022, in Dayton, Ohio, a USPS Letter Carrier was robbed at gun point of his USPS Arrow Key. Within hours of the robbery, law enforcement identified the getaway vehicle and getaway driver associated with this robbery. When arrested, the getaway driver had in his possession a cellular telephone. Through later interviews with the getaway driver, he admitted having his cellular device with him at the time of the robbery; a subsequent search of the cellular device confirmed his admission as it contained a video of the getaway driver and his accomplices in the getaway vehicle around the time of the robbery.

c. On or about March 31, 2023, Oakwood Police Department conducted a traffic stop of a vehicle and during the incident recovered stolen mail as well as the stolen Arrow Key from the November 26, 2022, robbery described above. Notably, both suspects in the vehicle had in their possession cellular devices; the arrow key, in fact, was recovered in the protective casing surrounding the cellular device. Again, this incident demonstrates that individuals involved in mail-related crimes tend to carry cellular devices with them during these incidents.

d. On October 21, 2023, in Cincinnati, Ohio, an USPS Letter Carrier was again robbed at gun point. On October 30, 2023, postal inspectors executed a residential search warrant at the home of a suspect in the robbery and recovered, among other things, a cellular device that belonged to him. A subsequent search of that device revealed that he had possessed it around the time of the robbery and used it to facilitate the crime. For instance, he sent a text message to a co-conspirator coordinating a ride to the robbery. He also sent other messages on the device indicating that it was easy to rob mailman. Once more, an investigation revealed that a robber possessed a cellular device during and in relation to an incident.

8. Additionally, based on my discussions with other law enforcement officers as well as my own experience, I know that the type of information requested in this warrant has led to the identification of suspects in other robbery incidents. For instance, the collection of this type of data will assist law enforcement identify cellular telephone numbers that have no known association with a particular location, which allows for potential identification of suspects who have just entered the area. Also, the type of information when collected from multiple robbery incidents will allow law enforcement to determine whether the same cellular devices were located at multiple robberies across a geographic area. If the same cellular telephone number appears at multiple robberies, it tends to suggest that the same person is involved in these incidents.

9. These principles apply to the December 18, 2023, incident as well. The location surrounding the robbery was a lightly trafficked area. Video footage collected from residences at the time of and in the vicinity of the incident capture little to no vehicle traffic other than the getaway sedan. Moreover, the warrant seeks a limited geographic range – namely, fifty meters – and timeframe – a range totaling fifteen minutes – around the three locations at which investigators placed the suspect around the time of the robbery. If the suspect and/or the getaway driver was carrying a cellular telephone, that device should appear at each of the three locations. As detailed above, based on my training and experience, and familiarity with other robbery investigations, it is a common practice for robbers to carry cellular devices with them during an incident. The information sought therefore may provide evidence concerning the identity of the robber and his accomplices.

10. In my training and experience, I have learned that PROVIDERS are companies that provides cellular communications service to the general public. To provide this service,

many cellular service providers maintain antenna towers (“cell towers”) that serve and provide cellular service to devices that are within range of the tower’s signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data. When sending or receiving communications, a cellular device does not always utilize the cell tower that is closest to it.

11. Based upon my training and experience, I also know that each cellular device is identified by one or more unique identifiers. For example, with respect to a cellular phone, the phone will be assigned both a unique telephone number but also one or more other identifiers such as an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), an International Mobile Equipment Identity (“IMEI”), a Subscription Permanent Identifier (“SUPI”), and/or a Network Access Identifier (“NAI”). The types of identifiers assigned to a given cellular device are dependent on the device and the cellular network on which it operates.

12. Based on my training and experience, I know that cellular providers, such as PROVIDERS, routinely and in their regular course of business maintain historical records that allow them to determine which wireless devices used cellular towers on the cellular provider’s network to send or receive communications. For each communication sent or received via the wireless provider’s network, these records may include: (1) the telephone call number and unique identifiers of the wireless device that connected to the provider’s cellular tower and sent or received the communication (“the locally served wireless device”); (2) the cellular tower(s) on

the provider's network, as well as the "sector" (*i.e.*, face of the tower), to which the locally served wireless device connected when sending or receiving the communication; and (3) the date, time, and duration of the communication.

13. In my training and experience, I have also learned that certain PROVIDERS collect and retain Timing Advance information from mobile devices operating on their networks. The Timing Advance data is generated for a number of reasons to include user activity, network registrations, and other signaling information. The Timing Advance dataset includes a device's estimated distance from the tower in addition to latitude and longitude coordinates representing the networks estimated location of the device. I am aware that these same PROVIDERS possess the capability to conduct a search of a predefined area and produce a record which identifies all mobile devices where a Timing Advance derived latitude and longitude coordinate falls within the search area. AT&T, US Cellular, and T-Mobile refers to Timing Advance data as True Call data whereas Verizon refers to Timing Advance data as the Real-Time Tool ("RTT").

14. Based on my training and experience and the above facts, information obtained from cellular service providers such as PROVIDERS that reveals which devices used a particular cell tower (and, where applicable, sector) to engage in particular communications can be used to show that such devices were in the general vicinity of the cell tower at the time the communication occurred. Thus, the records described in Attachment A will identify the cellular devices that were in the vicinity of the locations further identified in Attachment A at the time prior to and during the USPS Letter Carrier was being robbed, and during the time the suspect attempted to gain access to the USPS Vehicle. This information, in turn, will assist law enforcement in determining which person(s) were present at the target locations during the timeframes specified in Attachment A.

15. The government will utilize various methods to analyze the data produced by PROVIDERS in an effort to isolate mobile devices of interest while attempting to mitigate any undue invasion of privacy to innocent third parties. These analysis techniques include identifying devices that are common to two or more locations, isolating devices that are unique to an area specific to the date and time of the crime, or other methodologies in an effort to identify the device or devices which correspond to the known fact patterns of the investigation.

AUTHORIZATION REQUEST

16. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c).

17. I further request that the Court direct PROVIDERS to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on PROVIDERS, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

18. Your affiant knows through training and experience that individual's cellular telephones are commonly in the physical possession of owners which would yield information as to who was in the immediate area of the robberies within the timeframe identified related to each occurrence. Through the authorization of this Federal search warrant, the data will aid in the identification of devices contained in the area outlined in Attachment A to further the investigation into the identification of a suspect(s).

CONCLUSION

19. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

20. I further request that the Court direct the PROVIDERS to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on the PROVIDERS, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Joseph Rossiter

Joseph L. Rossiter
Postal Inspector
US Postal Inspection Service

Subscribed and sworn to before me on January 4, 2024


Peter B. Silvain, Jr.
United States Magistrate Judge


ATTACHMENT A

Property to Be Searched

A. Records and information associated with True Call Timing Advance area search(es) for all records of mobile devices which are determined to be present within the specified geographic location boundaries based upon the Timing Advance estimated geocoordinates for each respective mobile device that falls within the authorized date and time range provided below:

- All devices estimated to be within a **50-meter** radius of Location 1 (**Suspect staging**): **1286 Honeybee Dr, Dayton, OH 45417**, further identified by geocoordinates **39.76555, -84.826749** from **December 18, 2023 at 10:20 A.M. EASTERN** to **December 18, 2023 at 10:25 A.M. EASTERN**.
- All devices estimated to be within a **50-meter** radius of Location 2 (**Robbery Location**): **4808 Marburn Ave, Dayton, OH 45417**, further identified by geocoordinates **39.76530, -84.26846** from **December 18, 2023, at 10:25 A.M. EASTERN** to **December 18, 2023, at 10:30 A.M. EASTERN**.
- All devices estimated to be within a **50-meter** radius of Location 2 (**Attempted vehicle break-in**): **1350 Honeybee Dr, Dayton, OH 45417**, further identified by geocoordinates **39.76642, -84.26752** from **December 18, 2023, at 10:25 A.M. EASTERN** to **December 18, 2023, at 10:35 A.M. EASTERN**

The following cellular service provider(s) are required to disclose information to the United States pursuant to this warrant:

1. T-Mobile, a cellular service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.
2. AT&T, a cellular service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408.
3. US Cellular, a cellular service provider headquartered at 8410 West Bryn Mawr Ave., Chicago, IL 60631.

B. Records and information associated with RTT Timing Advance area search(es) for all records of mobile devices which are determined to be present within the specified geographic location boundaries based upon the Timing Advance estimated geocoordinates for each respective mobile device that falls within the authorized date and time range provided below:

- All devices estimated to be within a **50-meter** radius of Location 1 (**Suspect staging**): **1286 Honeybee Dr, Dayton, OH 45417**, further identified by geocoordinates **39.76555, -84.826749** from **December 18, 2023 at 10:20 A.M. EASTERN** to **December 18, 2023 at 10:25 A.M. EASTERN**.
- All devices estimated to be within a **50-meter** radius of Location 2 (**Robbery Location**): **4808 Marburn Ave, Dayton, OH 45417**, further identified by geocoordinates **39.76530, -84.26846** from **December 18, 2023, at 10:25 A.M. EASTERN** to **December 18, 2023, at 10:30 A.M. EASTERN**.
- All devices estimated to be within a **50-meter** radius of Location 2 (**Attempted vehicle break-in**): **1350 Honeybee Dr, Dayton, OH 45417**, further identified by geocoordinates **39.76642, -84.26752** from **December 18, 2023, at 10:25 A.M. EASTERN** to **December 18, 2023, at 10:35 A.M. EASTERN**

The following cellular service provider is required to disclose information to the United States pursuant to this warrant:

1. Verizon, a cellular service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

For each location described in Attachment A, the cellular service providers identified in Attachment A are required to disclose to the United States records and other information (not including the contents of communications) about all communications and signaling information to or from any cellular tower(s) where the mobile device is estimated to be located within the search parameters defined in Attachment A, including records that identify:

- a. the unique identifiers for each mobile device estimated to fall within the search area (“the located mobile device”), including Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), International Mobile Equipment Identities (“IMEI”), a Subscription Permanent Identifier (“SUPI”), and/or a Network Access Identifier (“NAI”);
- b. for each communication or signaling event, the “sector(s)” (i.e. the face(s) of the tower(s)) that sent or received a radio signal from the located mobile device, and the distance that the mobile device is estimated to be from the tower;
- c. the date, time, duration, and type of each communication or signaling event.

These records should include records about communications that were initiated before or terminated after the timeframe(s) identified in Attachment A if some part of the communication occurred during the relevant timeframe(s) listed in Attachment A.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Section 2114(a) during the period from December 18, 2023, at 10:20 a.m. through and including December 18, 2023, at 10:35 a.m.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

The government will utilize various methods to analyze the data produced by PROVIDERS in an effort to isolate mobile devices of interest while attempting to mitigate any undue invasion of privacy to innocent third parties. These analysis techniques include identifying devices that are common to two or more locations, reviewing records to locate devices associated with a known event (i.e. an offender observed answering a phone call on surveillance video with a corresponding date and time stamp), isolating devices that are unique to an area specific to the date and time of the crime, or other methodologies in an effort to identify the device or devices which correspond to the known fact patterns of the investigation.